NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

North Dakota

Nothing Significant to Report

Regional

(Minnesota) **Prairie Island plant declares 'unusual event.** Xcel Energy Inc. said its Prairie Island nuclear plant near Red Wing, Minnesota, declared an —unusual event after some security equipment failed October 31. The utility said the event happened around 2:15 p.m. and was declared over just before 6 p.m. Plant officials made the declaration after some security equipment temporarily failed. The equipment was restored, and plant officials were investigating the cause. The plant maintained security during the event. Xcel said it notified federal, State, and local officials. An unusual event declaration is the lowest of four emergency classifications. Source: http://www.kare11.com/news/article/996654/396/Prairie-Island-plant-declares-unusual-event

Drought influencing Missouri River management plan. Residents and officials in the Dakotas urged the U.S. Army Corps of Engineers to conserve water in upstream Missouri River reservoirs as drought conditions persist, the Associated Press reported October 31. The call comes just a year after record flooding on the river. The Corps would hold 6 meetings in 5 States over 4 days on its annual operating plan for the river for the upcoming year. Meetings were held October 25 in Bismarck, North Dakota, and Pierre, South Dakota. The Corps said September runoff in the Missouri River system was a record low. The National Oceanic and Atmospheric Administration said the dry conditions could carry into the spring. The Corps will conduct checks in March and July to determine what level of water to release to downstream areas. Source: http://www.timesunion.com/default/article/Drought-influencing-Missouri-River-management-plan-3996019.php

National

(New York) **Over 1.3M customers still without power in NYS.** The Long Island Power Authority (LIPA) said it expects to restore the majority of customers who lost power in New York by the weekend of November 10. There were more than 436,000 LIPA customers still without service as of November 2. LIPA said it was focusing on restoring power along main roads, traffic signals, and schools. In Manhattan, 226,000 buildings, homes, and business remained without power. Consolidated Edison said they should have service restored by November 3. It will take another week — in some cases 2 weeks — to restore power to the outer boroughs and northern suburbs, including Westchester, where over 140,000 remain without power. More than 1.3 million remained without power in New York State. Source: http://online.wsj.com/article/AP0f9a7cba2124433e9c5d9d72ec2b1c5c.html

ICS-CERT warns of increasing threat to industrial control systems. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued a warning about special tools and search engines that make attacks on systems and devices in infrastructures simple even for inexperienced attackers. Tools aimed at cracking digital control systems from companies such as GE, Rockwell Automation, Schneider Electric, and Koyo were released earlier in 2012. Tools for CoDeSys software from 3S Software also recently appeared. These tools lower the barriers for attackers by removing the need for specialist knowledge in order to carry out an attack. Special search engines such as the Shodan Computer Location Service and the Every Routable IP Project (ERIPP) are also making attacks simpler for attackers. One team of researchers told ICS-CERT that they used Shodan to discover more than 500,000 unsecured devices which use supervisory control and data acquisition (SCADA) and other industrial control systems (ICS). Source: http://www.h-online.com/security/news/item/ICS-CERT-warns-of-increasing-threat-to-industrial-control-systems-1739808.html

International

Nothing Significant to Report

Banking and Finance Industry

(California) **U.S. power market regulator seeks $470 million from Barclays.** U.S. federal energy regulators threatened to fine U.K. bank Barclays roughly $470 million to settle allegations that the bank and four traders manipulated California energy markets from November 2006 to December 2008, Reuters reported October 31. In a potentially record penalty that could eclipse fines over rigging the inter-bank lending rate known as Libor, the U.S. Federal Energy Regulatory Commission (FERC) said Barclays has 30 days to show why it should not be penalized for an alleged scheme of manipulating physical electricity markets in order to benefit from related positions in the swaps market. Barclays reiterated that it —strongly disagreed with the findings and was ready to fight the order. The FERC order suggests the agency was unable to reach a settlement with Barclays through negotiations, indicating the issue is likely to head toward an administrative court, said an expert in energy trade regulation. Source: http://www.reuters.com/article/2012/10/31/us-barclays-ferc-idUSBRE89U1QV20121031

IRS warns of sophisticated phishing scheme using fake IRS website. A sophisticated phishing scheme that uses an official-looking but fake Internal Revenue Service (IRS) Web site has been netting victims, the IRS said November 1. The scam uses a Web site that mimics the IRS e-Services registration page to collect personal information. The official page provides products for tax preparers, not the general public. —The phony Web page looks almost identical to the real one, the IRS said in a prepared statement. —Criminals use these sites to lure people into providing personal and financial information that may be used to steal the victim's money or identity. Source: http://blog.al.com/businessnews/2012/11/irs_warns_of_sophisticated_phi.html

Bank of America customers under phishing attack. The phishing —account suspended warning purportedly sent by Bank of America‘s Cardmember Services is hitting inboxes once again, Help Net Security reported October 31. —During our usual security enhancement protocol, we observed multiple login attempt error while login in to your online banking account, the email reads. ―We have believed that someone other than you is trying to access your account for security reasons, we have temporarily suspend your account and your access to online banking and will be restricted if you fail to update. According to PhishTank, the offered link takes potential victims to a very realistically spoofed Bank of America login page. The fake Web page has since been made unavailable. However, the URL in the email can be easily changed to point to another page, Source: http://www.net-security.org/secworld.php?id=13877

Barclays hit by fresh U.S. investigations. Barclays, already rocked by an interest rate rigging scandal, unveiled new U.S. regulatory investigations into the bank's financial probity October 31. Following investigations in the U.K. over its dealings with Qatari investors, Barclays said the U.S. Department of Justice and Securities and Exchange Commission were probing whether its relationships with third parties who help it win or retain business are compliant with U.S. laws. The bank is under investigation by Britain's financial regulator and fraud prosecutor into payments to Qatari investors after it raised billions of pounds from the Gulf state 5 years ago to save it from taking a taxpayer bailout. Barclays also said that the U.S. Federal Energy Regulatory Commission (FERC) could be close to fining it over an investigation into the manipulation of power prices in the western United States from late 2006 until 2008. FERC could notify the bank of proposed penalties as early as October 31, and Barclays said it would ―vigorously defend this matter. The investigation was first announced in April, alleging the bank took substantial electricity market positions to move daily index settlements. Source: http://www.reuters.com/article/2012/10/31/us-barclays-results-idUSBRE89U0C420121031

Bank phishing gang arrested after hotel swoop. U.K. police arrested three men accused of being involved in large-scale Trojan phishing attacks against a range of banks, Techworld reported October 30. Picked up in a London hotel after an operation described as ―intelligence-led , the two unnamed Romanians and a Nigerian were arrested October 29 on suspicion of money laundering and conspiracy to defraud, police said. The men are alleged to be behind the appearance of 2,000 bogus bank login pages that had been part of a campaign to steal account details. The police press release did not go into much detail beyond confirming that the attacks had hit a sizable number of bank users, leading to the theft of money. Computers were seized while further searches are being carried out in London and the Midlands. Source: http://news.techworld.com/security/3408031/bank-phishing-gang-arrested-after-hotel-swoop/

Chemical and Hazardous Materials Sector

(Illinois) **NRC raises concerns about Dresden flood plan.** The Nuclear Regulatory Commission (NRC) said it has questions about Exelon Generation's plan for handling a big flood at the Dresden Nuclear Station in Morris, Illinois, the Associated Press reported November 2. The commission that recent inspections raised concerns about whether the current plans are adequate in the event of a catastrophic flood like the one that swamped the Fukushima Daiichi plant in Japan in 2011. Among the questions is how the company would reach the plant to refuel a diesel pump that would circulate water to cool the reactor. The company has 30 days to respond. A NRC spokeswoman said the plan needs to address the worst possible flood, no matter how improbable. She said concerns with Dresden‘s plan do not represent an immediate safety risk. Source: http://newsok.com/nrc-raises-concerns-about-dresden-flood-plan/article/feed/457020

Commercial Facilities

Nothing Significant to Report

Communications Sector

Why many didn't get wireless emergency alerts during Sandy. Notifications alerting the public about Hurricane Sandy were what the Federal Emergency Management Agency (FEMA) and the Federal Communications Commission (FCC) call wireless emergency alerts, or WEAs, WLS 890 AM Chicago reported November 1. They were designed to alert people via their phones about three types of emergencies — imminent threats (including extreme or severe weather), AMBER alerts, and presidential alerts (alerts issued by the president). The alerts were launched in 2011 in many parts of the country and in May, came to AT&T, Verizon, Sprint, and other carriers. ―We have close to 100 carriers that are providing the service,   the vice president of regulatory affairs for the CTIA, the wireless industry trade group, told ABC News. He said that users can disable the imminent and AMBER alerts, but not the presidential ones. Source: http://www.wlsam.com/Article.asp?id=2564881&spid=

FCC: 25% of cell towers, broadband down in 10 States. Telecommunications companies told federal regulators that Hurricane Sandy knocked out 25% of wireless cell towers and a quarter of cable services in 10 States. A ―very small,   but unspecified, number of 9-1-1 call centers have also been affected, but emergency calls are being rerouted, the Federal Communications Commission (FCC) chairman told reporters October 30. Neither the telecom firms, which voluntarily reported the figures, nor the FCC estimated how many wireless and cable customers were affected. However, the FCC chief warned that service would likely get worse before it gets better. Further disruptions are expected as the storm moves west and north or if cell towers running on backup generators go down before electrical power is restored. Utility companies estimated that between 7 million and 8 million customers did not have power. Verizon Wireless, AT&T, Sprint Nextel, and T-Mobile USA all reported service problems, as did Cablevision Systems, Comcast, and Time Warner Cable. Source: http://www.usatoday.com/story/news/nation/2012/10/30/hurricane-sandy-wireless-cellphone-outage/1669921/

Hurricane Sandy disrupts Northeast US telecom networks. Verizon Communications said October 30 that its wireline service was suffering as flooding in its central offices in lower Manhattan affected its back-up generators and batteries. The company said that its engineers were on site October 29 and were beginning to assess damage. Sprint Nextel said it was seeing outages at some cell sites because of the power outages across all the States in Sandy's path including New York, New Jersey, Connecticut, Pennsylvania, Washington D.C., Maryland, northern Virginia, and New England. People complained of outages to their cable telephone, Internet, and television services from providers ranging from Comcast Corp, Cablevision Systems Corp, and Verizon in New Jersey, Connecticut, and New York. Cablevision said it was experiencing widespread service interruptions primarily related to loss of power. Cell phone service also appeared to be spotty for other top providers AT&T Inc and T-Mobile USA, a unit of Deutsche Telekom, according to some customers. Source: http://www.reuters.com/article/2012/10/30/uk-storm-sandy-telecommunications-idUSLNE89T02220121030

Critical Manufacturing

Ford website hacked by NullCrew, user credentials leaked online. The latest target of the hacker collective known as NullCrew was the Web site of car manufacturer Ford. The hackers claimed to have leveraged an SQL Injection vulnerability in order to gain access to the databases behind the social.ford.com subdomain. As a result of the breach, database and table names, customer usernames – represented by email addresses – and encrypted passwords were leaked. In total, 18 credential sets were published online. Most of the affected individuals appeared to be employed at an ad agency called Team Detroit. —No confidential information was compromised by the incident. Our teams have been working on determining how this happened and have changed all site passwords as a precaution, a Ford Global Digital Communications spokesman said. Source: http://news.softpedia.com/news/Ford-Website-Hacked-by-NullCrew-User-Credentials-Leaked-Online-302688.shtml

NHTSA recall notice - BMW 7-Series automatic transmission control module. BMW is recalling 45,500 model year 2005-2008 7-Series vehicles, equipped with the Comfort Access option and manufactured August 23, 2004, through July 24, 2008. The affected vehicles have an electronic key and an electronic connection between the gear shifter and the transmission (shift-by-wire) that automatically shifts the transmission to Park when the driver presses the Start/Stop button to shut down the engine. If the driver presses the engine Start/Stop button 2 or 3 times within a short time interval, the system may shift the transmission to Neutral rather than Park. If using the electronic key (Comfort Access mode), there would be no protection from the ignition interlock that prevents key removal if the vehicle is not in Park. If the driver exits the vehicle with the transmission in Neutral and the parking brake is not applied, the vehicle may rollaway. Unattended rollaway incidents often result in a crash or cause injury to pedestrians attempting to stop or enter the vehicle or to other bystanders in the path of the vehicle. BMW will notify owners beginning in November 2012, but will not have revised software available to remedy the vehicles until March 2013. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V502000&summary=true&prod_id=204671&PrintVersion=YES

Defense/ Industry Base Sector

(New Mexico) **NNSA pledges to fix Los Alamos plutonium site defense system.** The Presidential administration said it would work to eliminate technical flaws in a developmental protective mechanism for the country's sole facility capable of producing key nuclear-bomb explosion initiator components, the Associated Press reported October 26. Defensive technology under preparation to guard the Technical Area 55 plutonium site continue to suffer from significant malfunctioning, the Los Alamos National Laboratory in New Mexico verified. Officials previously announced plans to indefinitely defer completion of the 7-year-old project that has absorbed $213 million in funding, according to earlier reporting. The National Nuclear Security Administration would dispatch specialists to the laboratory "to examine the financial and management issues that led us to this point," a spokesman for the agency said. Separate controversies focused on the potential for radioactive material to escape from the Los Alamos laboratory's aging PF-4 plutonium site, and on the spiking expense of the facility's Chemistry and Metallurgy Research Replacement Project. The Presidential administration is seeking to delay that initiative. Source: http://www.nti.org/gsn/article/nnsa-pledges-fix-lanl-plutonium-site-defenses/

Emergency Services

(Virginia) **Three bombs explode; source says detective and a family were targets.** Three pipe bombs exploded October 30 and sources close to the investigation said that a Stafford, Virginia detective and a Stafford family were the intended targets. Now multiple police sources claim the Feds and local law enforcement are searching for a former law school student in connection with the crimes. Fredericksburg Police and agents from the Bureau of Alcohol, Tobacco, Firearms, and Explosives spent more than half the day at the targeted home. —We had windows blown out, holes through the roof, and walls damaged in the house, said a Fredericksburg Police public information officer. Investigators said clues collected at that home led them to believe the same suspect was involved in two other bomb blasts. —We've determined they are connected, said the public information officer. Sources close to the investigation said a Stafford detective used to rent the home a couple of years ago but no longer lives at that address. A Stafford detective's home in another neighborhood was also hit with a pipe bomb about 35 minutes after the Fredericksburg bombing. The third house was hit by a pipe bomb blast October 30. The suspect planted a pipe bomb with bolts, screws, and nails inside. The bomb was wedged between sand bags the homeowner had been using to keep storm water out. Source: http://wtvr.com/2012/10/31/three-bombs-explode-source-says-detective-and-a-family-were-targets/

(California) **Fake mayday calls in O.C. send Coast Guard scrambling.** U.S. Coast Guard officials are trying to track down a man who has reported several fake distress calls in California regarding sinking ships, wasting time and money on rescue efforts, the Los Angeles Times reported October 29. Coast Guard officials said the fake distress calls divert help from people who really need it. During the week of October 22, a man that the Coast Guard tracked to Orange County, California made six calls over the radio. He has prompted two attempted rescues and said things like, "Mayday, mayday, my dog ate my homework," before he claims he is drowning or had some sort of accident. In the last hoax call October 26, the man said his boat was sinking in Newport Harbor. The Coast Guard deployed a vessel that costs $2,600 per hour and a helicopter that runs more than $8,600 per hour. In all, the 12 1/2-hour search cost taxpayers about $50,000, exhausted resources and, according to officials, potentially put other boaters at risk. Now investigators are trying to locate the man who is making the bogus calls. Source: http://latimesblogs.latimes.com/lanow/2012/10/fake-mayday-calls-in-oc-send-coast-guard-scrambling.html

Energy

Solar panels no savior in a blackout. Some of the roughly 6 million power customers in the northeast without electricity in Hurricane Sandy’s wake may be glancing around at a handful of homes with solar panels on their rooftops, thinking their clean-powered neighbors might have juice. However, most residential solar panels are connected to the power grid, according to the Solar Energy Industries Association, and when the grid goes down, so do they. One reason the grid-connected solar systems shut down automatically in outages is that when the power goes off, if home solar installations send electricity onto the lines, it could electrocute workers repairing them. In the U.S., it is also rare for residential solar customers to have batteries in their home to store the power coming off their roofs in case of a broader outage. Source: http://www.businessweek.com/articles/2012-10-31/solar-panels-no-savior-in-a-blackout

(New York) **1.9M customers still without power in NY State.** Utility crews in the Hudson Valley, New York continued their efforts to restore electricity service to the tens of thousands of customers still without power in the aftermath of superstorm Sandy. Most of the outages in Mid-Hudson Valley were in Dutchess, Orange, and Ulster counties, where more than 100,000 customers remained without power October 31. Sullivan County in southeast New York had another 32,000 outages. The power situation is even worse on Long Island and in New York City and its northern suburbs, where more than 1.6 million customers have lost power from the October 29 storm. In all, some 1.9 million utility customers in New York State have lost power because of Sandy. Utility officials say they are still assessing the damage in many areas and have given no estimates on when they expect power to be restored. Source: http://online.wsj.com/article/AP28202beab2424d3ea7bef5e5b22d2c01.html

(New Jersey) **More than 2M in NJ without electricity.** Utility crews were assessing the damage and working to restore service to more than 2 million homes and businesses in New Jersey. The State‘s largest utility, Public Service Electric & Gas (PSE&G), said it has restored power to 30 percent of its 1.4 million customers who lost service. Still, 900,000 PSE&G customers are without electricity. Jersey Central Power & Light reported outages for 954,283 customers, mainly in Monmouth and Ocean counties. Atlantic City Electric said 121,035 homes and businesses remain in the dark. Orange & Rockland Electric reported 53,822 customers without service. Source: http://www.abc27.com/story/19960011/more-than-2m-in-nj-without-electricity

Sandy cuts E. Coast fuel supply; refiners, pipelines shut. The supply of gasoline, diesel, and jet fuel into the East Coast ground almost to a halt October 29, as Hurricane Sandy forced the closure of two-thirds of the region's refineries, its biggest pipeline, and most major ports. Benchmark New York harbor gasoline futures jumped as much as 11 cents a gallon, with traders fearing that power outages and flooding could leave refiners struggling to restore operations after the broadest storm ever to hit the United States. With Sandy gaining strength as it nears the coast, refinery, pipeline, port, and terminal operators shuttered or reduced operations, increasing the risk that bottlenecks would keep supplies of motor and heating fuel from customers. Colonial Pipeline, the nation's largest oil products pipeline that connects the East Coast to Gulf Coast refiners, said it has shut down lines servicing individual terminals along the Northeastern seaboard. Nearly 70 percent of the region's refining capacity was on track to be idled. Source: http://www.reuters.com/article/2012/10/29/storm-sandy-refining-idUSL1E8LS1OU20121029

Food and Agriculture

CDC: 22 Illnesses and 4 deaths now linked to Listeria cheese. Two more cases were added to the multi-State outbreak of listeriosis linked to imported Frescolina Marte brand ricotta salata cheese, according to the Centers for Disease Control and Prevention (CDC). As of October 26, the CDC said a total of 22 persons infected with the outbreak-associated strain of Listeria monocytogenes were reported from 13 States and the District of Columbia. Of the known cases, 20 people were hospitalized; four deaths were reported. Listeriosis contributed to at least two of these deaths, according to the CDC's update. The agency also said that one fetal loss was reported. Source: http://www.foodsafetynews.com/2012/10/cdc-22-illnesses-and-4-deaths-linked-to-listeria-cheese/

Government Sector (including Schools and Universities)

(South Carolina) **Data security breach expands to 657K SC businesses; suit filed against State.** As many as 657,000 South Carolina businesses had their tax information stolen in the massive security breach at the South Carolina Department of Revenue that also claimed the records of up to 3.6 million people, the State's governor said October 31. Since October 26, when they announced the hacking publicly, State officials said they did not think business records were exposed. However, Mandiant, a consultant hired by the Department of Revenue, found that business tax records were compromised, too, the governor said. State officials were still learning more about the data theft, which is affecting four times as many people as all previous breaches combined in the State over the past 7 years. Like other taxpayers, businesses will be able to get free credit monitoring, but companies will get longer coverage. Source: http://www.thestate.com/2012/11/01/2503354/657000-sc-business-records-also.html#.UJJ-UG_A-NA

(South Carolina) **Hacker gained access to data using employee credentials.** South Carolina's identity theft nightmare has grown to include some businesses, and officials have disclosed for the first time that the hacker was able to crack the system by somehow obtaining the credentials of a Department of Revenue employee. The director of the Revenue Department disclosed October 29, about the possible impact of the breach on small businesses that an unspecified number of State identity numbers used for corporations had been —compromised at the same time as 3.6 million Social Security numbers and 387,000 mostly encrypted credit or debit card numbers. The director also disclosed October 30, that the hacker was able to breach the Revenue Department‗s system by somehow obtaining an employee‗s credentials. He said about 250 employees have special credentials that allow them access to the system. He declined to say whether the State knew whose credentials were used. The governor of South Carolina announced that the State had negotiated an agreement with Experian, which is providing identity theft protection and credit monitoring for taxpayers who have filed returns since 1998, to cap costs for taxpayers at $12 million. The director of the Revenue Department said 5,000 of the credit or debit card numbers exposed in the hacking are expired cards that cannot be used. Source: http://www.greenvilleonline.com/article/20121031/NEWS/310310036/Hacker-gained-access-to-data-using-employee-credentials?odyssey=tab|mostpopular|text|NEWS&nclick_check=1

(South Carolina) **Security breach could cost State more than $12 million.** The security breach that put millions of South Carolinians’ social security numbers and credit cards in jeopardy could cost the State more than $12 million in fees to companies that will be working to protect those citizens and investigate the data theft. The South Carolina governor said October 30 that the State negotiated a capped rate of $12 million with Experian, the company providing credit monitoring and lifetime fraud protection to those affected by the data breach. The State already paid $125,000 to Mandiant, which is investigating how the breach of the Department of Revenue’s servers happened and how to protect the State’s online systems in the future. The governor also noted that out the hundreds of thousands of credit card numbers that were taken, none of the unencrypted cards were active. Experts have told the State that it may take up to 6-8 months for those who have stolen social security numbers to start using them for fraudulent activity. Those same experts, according to the governor, said that after a year the likelihood for fraudulent activity goes way down. The governor said 533,000 people have called the hotline and 287,000 have signed up for the offered services. Source: http://www.wbtv.com/story/19951015/haley-security-breach-could-cost-state-more-than-12-million

(South Carolina) **Millions of South Carolinians' Social Security numbers stolen from State agency.** The South Carolina Department of Revenue's Web site was hacked and millions of social security numbers and credit and debit card numbers belonging to approximately 77 percent of South Carolina residents were compromised, WIS 10 Columbia reported October 28. State officials revealed that someone in a foreign country gained access to the Web site and a server was breached for the first time in late August. 387,000 credit and debit card numbers and 3.6 million Social Security numbers were exposed. The Social Security numbers were unencrypted. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under credit card industry standards, officials said. However, approximately 16,000 were unencrypted and exposed. Officials found out about the breach October 10. October 16, investigators uncovered two attempts to probe the system in early September, and later learned that a previous attempt was made August 27. In mid-September, two other intrusions occurred, and to the best of the department's knowledge, the hacker obtained data for the first time. No other intrusions were uncovered. October 20, the vulnerability in the system was closed and, to the best of the department's knowledge, secured. The breach potentially affects anyone who has paid taxes in South Carolina since 1998. Source: http://www.wbtv.com/story/19926154/social-security-breach-nikki-haley-south-carolina-credit-cards-hacker

Information Technology and Telecommunications

Cyber criminals look to exploit interest in Windows 8. Two cyber threats targeting early adopters of Microsoft's recently launched Windows 8 operating system were recently discovered. Trend Micro detected the TROJ_FAKEAV.EHM malware and a phishing email scam targeting Windows 8 customers October 31. The malware is reportedly hosted and spread via a number of malicious sites. It infects machines by displaying a fake scanning result window that aims to dupe its victims into purchasing a bogus antivirus program for Windows 8. The phishing email looks to fool users into handing over sensitive data, such as their email address and password, by masquerading as a fake, free Windows 8 download offer. Source: http://www.v3.co.uk/v3-uk/news/2221625/cyber-criminals-look-to-exploit-interest-in-windows-8

Researcher warns that 'zombie browsers' are skyrocketing. Some Web browsers can be tricked into using so-called malicious extensions that can give hackers the ability to hijack the user's session, spy on Web cameras, upload and download files, and in the newer mobile-device area, hack into Google Android phones. An IT security consultant at Deloitte Hungary spoke about the topic he calls —zombie browsers during the Hacker Halted Conference in Miami the week of October 29. He said up until a year ago, only 10 of these browser malicious extensions were known to exist, but 2012 has seen 49 new ones already. —It's skyrocketing, the consultant noted, and he faulted the antivirus vendors for allegedly not addressing the issue at all. —Even after two years, none of the antivirus vendors detect these, he said, saying he's issuing a plea for them —to try harder on detecting malicious extensions. In his talk, he explained how malicious extensions in Firefox, Chrome, and Safari have been created by attackers that try to get them added to the user's browser through Web-based drive-by downloads or infected attachments. The result might be giving the attacker a way to steal data or spy on users, he said. Source: http://www.computerworld.com/s/article/9233140/Researcher_warns_that_zombie_browsers_are_skyrocketing

Free Android apps often secretly make calls, use the camera. Freebie mobile applications come with a higher privacy and security risk, according to an 18-month long study by Juniper Networks. The networking company ran an audit of 1.7 million applications on the Android market and discovered that free applications are 5 times more likely to track user location and 314 percent more likely to access user address books than paid counterparts. Around 1 in 4 (24.1 percent) free apps require permission to track location, while only 6 percent of paid apps request this ability. Approximately 6.7 percent of freebie Android apps have permission to access user's address book, a figure that drops to just 2.1 percent for paid apps. It is commonly assumed that free apps collect information in order to serve advertisements from third-party ad networks. While this is true in some cases, Juniper found that the percentage of apps with the top 5 ad networks (9 percent) is much less than the total number tracking location (24.1 percent). Approximately 4.1 percent of apps feature ads from the AirPush network, with a total of nearly 5 percent of freebie Android apps linked to either the AdMob, Millennial Media, AdWhirl, or the Leadbolt ad networks. ―This leads us to believe there are several apps collecting information for reasons less apparent than advertising, Juniper said. Source: http://www.theregister.co.uk/2012/11/01/android_app_privacy_audit/

Cybercriminals continue to improve Skype-spreading malware. At the beginning of October, cybercriminals started spreading malware via Skype by using messages such as ―lol is this your new profile pic to trick users into clicking on malicious links. According to security firms, millions of users might have infected their computers after clicking on the suspicious links. Although the infection rates have dropped since, security researchers say the individuals responsible for developing and maintaining the threats known as W32.IRCBot.NG and W32.Phopifas have not given up on their project. The infection routine remains unchanged, but the developers added new hosts from which the pieces of malware can be downloaded, Symantec experts explain. Furthermore, W32.IRCBot.NG is capable of stealing passwords for file-hosting sites, and several new languages have been added to ensure that the malware can target a wider range of users. Some malicious modules have been placed on virtual server services and one of the URLs is even being listed in the Top 100 downloads section of a ranking Web site. Source: http://news.softpedia.com/news/Cybercriminals-Continue-to-Improve-Skype-Spreading-Malware-303654.shtml

SQL Injections and DDoS attacks: Most popular topics on hacker forums. Security solutions provider Imperva released the result of its 13th Hacker Intelligence Initiative report, which is based on the analysis of some highly popular hacker forums, including one that is considered to be one of the largest, with 250,000 members. According to experts, the most discussed topics on hacker forums are SQL Injection and distributed denial-of-service (DDoS) attacks, both occupying 19 percent of the discussion volume. It is believed SQL Injection is a favorite attack vector because many of the security solutions deployed by organizations do not even know how to identify such attacks. Another hot topic among hackers is represented by social networks. That is because these Web sites are not only an important source of information, but they also provide the means to make a profit. Facebook is the most discussed (39 percent), followed by Twitter (37 percent), and Myspace (15 percent). Google+ and LinkedIn show up in only 5 percent and 4 percent, respectively, of the social media-related threads. Source: http://news.softpedia.com/news/SQL-Injections-and-DDOS-Attacks-Most-Popular-Topics-on-Hacker-Forums-303268.shtml

Privacy-invading module found in thousands of apps on Google Play. An advertising module embedded into over 7,000 "free" fake versions of legitimate Android applications that can be found on Google Play is actively harvesting personal and mobile use information from unsuspecting users, warned a Trend Micro senior threat researcher. She detected one such app after downloading by mistake a fake Flash Player from Google's official Android market and getting warned about its malicious nature by her company's own mobile security app. After consulting with a colleague from the Mobile Application Reputation team, she discovered the extent of the problem: apart from pushing ads onto the users, the adware module inside the app also sends information such as device ID, OS version, IP address, and the user's phone number, GPS location, account information, calendar, and browser bookmarks to the servers of the company that created the module. This particular ad module compromises the users' privacy and their devices' usability. It was found in over 7,000 free apps offered on Google Play. "80% of them are still available, and at least 10% of them have been downloaded more than one million times," the researcher warned, and added that the Web of Trust community believes the company that created the module is also involved in phishing and scamming users. Source: http://www.net-security.org/secworld.php?id=13860

National Monuments and Icons

(New York) **Statue of Liberty closes indefinitely after superstorm Sandy.** The Statue of Liberty shut down October 29 as a result of superstorm Sandy, a day after its grand reopening. —Due to conditions created by Hurricane Sandy, Statue of Liberty National Monument will be closed until further notice, the alert on the National Park Service Web site read. The Statue of Liberty Facebook pages stated, —The Statue of Liberty National Monument, encompassing both Liberty and Ellis Islands, will be CLOSED through Saturday, November 3rd. Please refer to our FB page and our Twitter feed @StatueLibrtyNPS for information regarding plans for Sunday. Our maintenance crews have a huge challenge in pumping water and clearing debris from the islands, but the conditions at the screening facilities in Battery Park, NY, and Liberty State Park, NJ, will also affect operations. Source: http://www.kabc.com/rssItem.asp?feedid=118&itemid=29933799

Postal and Shipping

Nothing Significant to Report

Public Health

Nine more cases of meningitis reported in outbreak. Nine more cases of deadly fungal meningitis were reported from an outbreak tied to steroid medications shipped by a Massachusetts company, bringing the national total to 377 cases, U.S. health officials said November 1. The Centers for Disease Control and Prevention (CDC) said Virginia revised down the number of deaths from three to two, reducing the national fatality total to 28. The CDC gave no reason for the revision. In addition to the 377 cases of meningitis, the CDC said there also were 9 reported cases of infections after a potentially contaminated steroid was injected into a joint such as a knee, hip, shoulder, or elbow, bringing the total number of infections nationwide to 386. The steroid was supplied by New England Compounding Center of Massachusetts, which faces multiple investigations. Health authorities said its facility near Boston failed to make medications in sterile conditions. Source: http://news.yahoo.com/nine-more-cases-meningitis-reported-outbreak-233744039.html

Investigation faults handling of Medicare patient data breaches. In October, the Department of Health and Human Services' Office of the Inspector General (OIG) published a report of its investigation of Centers for Medicare & Medicaid Services' management of a database of Medicare identification numbers, for patients and physicians, which were compromised because of a breach. The report found that Medicare was not doing enough to mitigate damages caused when a Medicare patient's identification is stolen. The OIG found a need for better management of the database and consistency in how Medicare contractors use the database to catch and prevent fraud. The lack of consistency could cause a disruption in payments to physicians and other health care organizations that treat and provide medical supplies to Medicare patients. The OIG examined 14 breaches affecting 13,755 beneficiaries that occurred between September 23, 2009, when the notification rules under the economic stimulus package went into effect, and December 31, 2011. Of the 14 breach cases, the OIG found that: Notification was not made within the required 60 days in seven cases; Notification did not include a description of the breach investigation, loss mitigation, and protection against further breaches in six cases; Notification did not include when breaches occurred or were discovered in seven cases; Notification did not include the breached information, contact procedures, or steps to protect from harm in three cases. Source: http://www.ama-assn.org/amednews/2012/10/29/bisb1029.htm

Transportation

$12 million DOT emergency relief funds released for Hurricane Sandy damage. The U.S. Transportation Secretary announced he was making $12 million in quick release emergency relief funds immediately available to New Jersey and Connecticut to help begin repairing the damage caused by Hurricane Sandy, while assessments continued throughout the Northeast to determine the full extent of the damage, Heavy Duty Trucking Magazine reported November 2. The announcement followed the U.S. President's call for federal agencies to act quickly and bring all available resources to bear as quickly as possible. It also builds on the disaster assistance efforts the Presidential administration approved the week of October 29, including major disaster declarations, which make federal assistance — like these emergency relief funds — available to supplement State and local response and recovery efforts. The funds — $10 million for New Jersey and $2 million for Connecticut — mark another installment of federal-aid highway funds going toward repairing damage from Hurricane Sandy. The week of October 29, the Department of Transportation approved $17 million in quick release emergency relief funds — $10 million for New York; $3 million for Rhode Island; and $4 million for North Carolina. New Jersey will use the funding to help maintain essential traffic flow and repair sections of highway necessary to prevent further damage; Connecticut will use it for general emergency repairs to federal aid highways. Source: http://www.truckinginfo.com/news/news-detail.asp?news_id=78454

Improving high-speed rail ties against freezing, thawing conditions. A research project is helping high-speed rail systems handle the stress of freezing and thawing weather conditions, Homeland Security News Wire reported October 31. The 3-year study looks at the freeze-thaw durability of concrete railroad ties. A Kansas State University release reports that the Federal Railroad Association recently awarded more than $1.2 million for the study of the materials and fabrication process, and to develop quality control tests that ensure safe freeze-thaw durable concrete railroad ties. To study the freeze-thaw conditions in concrete rail ties, researchers will add surfactants to the concrete as it is being mixed in the laboratory. These compounds produce millions of microscopic bubbles in the concrete that act as pressure release valves to help protect the concrete against damage. Researchers will evaluate the vibration conditions and air voids created by the bubbles in rail ties produced from various other materials, including surrogate clear materials, cement paste, and mortars before scaling up to concrete. The ties will also be studied to determine if they get wet enough on the tracks to cause damage. Additionally, the team will develop evaluation methods that will help railroad tie manufacturers determine the freeze-thaw resistance of concrete rail ties once they are produced. Source: http://www.homelandsecuritynewswire.com/dr20121030-improving-highspeed-rail-ties-against-freezing-thawing-conditions

(Michigan) **Driver wounded in interstate shooting.** A motorist driving along Interstate 96 was shot and wounded October 27 in the latest in a string of shootings in southeastern Michigan. A Livingston County sheriff said the Delton man was taken to the hospital for a gunshot wound in the left buttock area by a bullet that came through the door. He was listed in stable condition at a hospital. The sheriff said shots were fired into another car earlier, but the two people inside were not hurt. A specially-formed task force with dozens of investigators has been working to solve 24 reported shootings along the interstate, or near it, in Ingham County, Oakland County, Livingston County, and Shiawassee County. Ten of the incidents happened in Wixom alone. No one was hurt in any of the previous shootings. Source: http://www.abc-7.com/story/19941973/driver-wounded-in-interstate-shooting

Water and Dams

$56M awarded for dam repairs. The Army Corps of Engineers awarded the final round of contracts for repairs throughout the Missouri River basin following the flood of 2011, the Glasgow Courier reported November 1. The final repair bill for the Corps' Omaha District totaled $360 million. Levee rehabilitation work came to $160 million and repairs to damages at the six mainstem dam projects totaled $200 million. The work on 15 levee systems is expected to be complete by the spring of 2013. Completion of work on the dams will take a year or more. According to a release from the Omaha District, examples of repair work include spillway repairs, under seepage control systems, repairs to Corps-owned levees that were scoured during the flood, relief wells, retaining walls, toe drains, and other erosion repairs. Six projects totaling more than $56 million were awarded for construction at the Fort Peck Dam and power plant. The Fort Peck Project manager said several of the contracts were multi-year repairs scheduled for completion in 2015. Source: http://www.glasgowcourier.com/cms/news/story-654901.html

(New Jersey) **NJ inspectors determine cause of Meadowlands flooding.** The dozens of tide gates, berms, and levees in the Meadowlands were no match for the record-high surge of sea water propelled by Hurricane Sandy that devastated Moonachie, Little Ferry, and other low-lying towns along the Hackensack River in New Jersey, the Bergen Record reported October 31. State officials October 31 said the water was so high it poured over all the anti-flooding devices in the region. A record surge of 11.9 feet was set October 29 at the mouth of the Hackensack River in Newark, according to National Weather Service data. A combination of gale-force winds, high tides, and a full moon pushed a wall of water from the Atlantic Ocean into Newark Bay and then up the Hackensack and into its tributaries. About 90 percent of the 14-town region is two feet or less from the mean high-water mark. More than 5,000 homes and 2,000 businesses fall within a Federal Emergency Management Agency special flood hazard area. The Meadowlands has dozens of tide gates, pump stations, drainage ditches, levees, and berms to control flooding in the area, one of New Jersey's largest marshlands. However, many of those structures are decades old, having been battered by the elements so much that they are no longer effective. Source: http://www.northjersey.com/news/Officials_Surge_of_water_from_Hurricane_Sandy_record-breaking_at_Meadowlands.html?page=all

(New York) **New York American Water asks customers to conserve water after Hurricane Sandy.** As New York recovered from Hurricane Sandy, New York American Water urged its customers to conserve water as many of the company's facilities were operating on emergency generators, Business Wire reported October 31. In the aftermath of the storm, water service for New York American Water customers was not interrupted and the company did not issue any boil water advisories. —We are working with the power companies to have power fully restored at all of our pumping stations and water treatment plants, and ask that our customers discontinue non-essential water use until further notice, said the president of New York American Water. —Voluntary water conservation reduces the demand on the water system while it operates on backup power. Source: http://www.businesswire.com/news/home/20121031005956/en/York-American-Water-Asks-Customers-Conserve-Water

(Washington) **Bomb destroys flood gauge on eve of storm.** A witness heard an explosion near his home in Pacific, Washington, October 28 that turned out be some kind of homemade explosive that destroyed an important U.S. Geological Survey (USGS) flood monitoring device on the flood prone White River. The device uplinks critical river flow information to the Web for flood managers from several agencies. The U.S. Army Corps of Engineers used it for the operation of the Howard Hanson Dam upstream. The agencies were expecting to use it during the upcoming rain storms forecasted for October 30 and the rest of the week. The box is so vital for flood protection that USGS technicians replaced it in a matter of a few hours. Pacific police were not commenting on the case, but did say they have not arrested anyone and have no suspects at this time. The boxes provide a network that give agencies an overall flood picture so they can evacuate homes and close streets if necessary hours before the flood waters arrive. Source: http://www.nwcn.com/home/?fId=176356601&fPath=/news/local&fDomain=10212

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168